CLAIMS

1. An information input/output system comprising:

an input/output device; and

an information usage device that performs information input/output via the input/output device, wherein

the input/output device has the information usage device perform part of processing for judging whether the information usage device is one of valid and revoked.

2. The information input/output system of claim 1, wherein:

the input/output device outputs an identifier list to the information usage device, the identifier list including one or more identifiers, arranged according to a predetermined rule, that each correspond to a different valid or revoked device,

the information usage device, as part of the judgment processing, uses the received identifier list in specifying a target range that includes a target identifier stored by the information usage device, and outputs range information indicating the specified target range to the input/output device, and

the input/output device receives the range information from the information usage device, and uses the received range information in judging whether the information usage device is valid or revoked.

3. The information input/output system of claim 2, wherein

the input/output device includes:

an acquiring unit operable to acquire the identifier list from an external source;

an output unit operable to output the acquired identifier list to the information usage device;

an ID receiving unit operable to receive from the information usage device, the target identifier and, as the range information, one or more identifiers from the identifier list that are included within the target range; and

a judging unit operable to judge whether the information usage device is valid or revoked, depending on whether the received target identifier matches any of the identifiers received as the range information, and to suppress the information input/output if the information usage device is judged to be revoked, and

the information usage device includes:

a storage unit operable to store the target identifier, which corresponds to the information usage device;

a receiving unit operable to receive the identifier list from the input/output device;

an extracting unit operable to use the received identifier list in specifying the target range, and to extract all of the identifiers included within the specified target range from the identifier list; and

a data output unit operable to output to the input/output device the target identifier and the one or more identifiers extracted as the range information.

4. The information input/output system of claim 3, wherein

the extracting unit specifies the target range from one or more ranges each defined by two identifiers arranged consecutively in the identifier list, and extracts the two identifiers defining the specified target range,

the data output unit outputs to the input/output device the target identifier and the two identifiers extracted as the range information,

the ID receiving unit receives from the information usage device the target identifier and the two identifiers extracted as the range information, and

the judging unit judges whether the information usage device is valid or revoked, depending on whether the target identifier matches either of the two extracted identifiers.

5. The information input/output system of claim 3, wherein

the target identifier identifies a public-key certificate certifying the authenticity of a public key of the information usage device,

each identifier in the identifier list identifies a public-key certificate of a different revoked device,

the extracting unit extracts in the arranged order, the one or more identifiers included within the specified target range, and

the judging unit judges the information usage device to be revoked if the target identifier matches any of the one or more extracted identifiers, and to be valid if the target identifier does not match any of the one or more extracted identifiers.

6. The information input/output system of claim 5, wherein

the identifier list has arranged therein according to the predetermined rule, certification data that certifies, with respect to each of one or more ranges, the authenticity of the one or more identifiers included within the range,

the extracting unit extracts from the identifier list, the certification data certifying the authenticity of the one or more extracted identifiers,

the data output unit outputs the extracted certification data to the input/output device,

the ID receiving unit receives the extracted certification data from the information usage device, and

the judging unit verifies the authenticity of the received certification data, and judges, if the authenticity is verified, whether the information usage device is valid or revoked.

7. The information input/output system of claim 3, wherein

the target identifier identifies a public-key certificate certifying the authenticity of a public key of the information usage device,

each identifier in the identifier list identifies a public-key certificate of a different valid device,

the extracting unit judges whether any of the identifiers in the identifier list match the target identifier, and extracts the matching identifier if judged in the affirmative, and

the judging unit judges the information usage device to be valid if the target and extracted identifiers match.

8. The information input/output system of claim 7, wherein

the identifier list has arranged therein one or more pieces of certification data, each corresponded to and certifying the authenticity of a different one of the identifiers,

the extracting unit extracts the certification data corresponding to the extracted identifier,

the data output unit outputs the extracted certification data to the input/output device,

the ID receiving unit receives the extracted certification data from the information usage device, and

the judging unit verifies the authenticity of the received certification data, and judges, if the authenticity is verified, whether the information usage device is valid or revoked.

9. The information input/output system of claim 3, wherein

the input/output device further includes:

an information output unit operable to securely output usage information to the information usage device, if the information usage device is judged to be valid, and

the information usage device further includes:

a usage unit operable to securely receive the usage information from the input/output device, and use the received usage information.

10. The information input/output system of claim 3, wherein

the input/output device further includes:

an ID storage unit operable to store a certificate identifier that identifies a public-key certificate certifying the authenticity of a public key of the input/output device; and

an ID output unit operable to output the certificate identifier to the information usage device, and

the information usage device further includes:

an ID reception unit operable to receive the certificate identifier from the input/output device;

a list receiving unit operable to receive a revocation list via the input/output device, the revocation list including one or more revoked identifiers that each identify a public-key certificate of a different revoked device; and

an ID judging unit operable to judge whether the input/output device is valid or revoked, depending on whether the received certificate identifier matches any of the revoked identifiers included in the revocation list.

11. The information input/output system of claim 10, wherein

the input/output device further includes:

a 1st processing unit operable to establish a secure communication channel between the input/output device and the information usage device, if the information usage device is judged to be valid; and

an information output unit operable to securely output usage information to the information usage device, if the secure communication channel is established, and

the information usage device further includes:

a 2nd processing unit operable to establish a secure communication channel between the information usage device and the input/output device, if the input/output device is judged to be valid; and a usage unit operable to securely receive the usage information from the input/output device if the secure communication channel is established, and to use the received usage information.

12. The information input/output system of claim 3 further comprising a recording medium storing the identifier list, wherein

the acquiring unit acquires the identifier list from the recording medium.

13. The information input/output system of claim 3 further comprising a communication medium operable to receive the identifier list, wherein

the acquiring unit acquires the identifier list from the communication medium.

14. The information input/output system of claim 3 further comprising a list generation device that includes:

a list storage unit; and

a generating unit operable to generate the identifier list, and write the generated identifier list to the list storage unit.

15. An input/output device via which an information usage

device performs information input/output, and that has the information usage device perform part of processing for judging whether the information usage device is one of valid and revoked.

16. The input/output device of claim 15 outputs an identifier list to the information usage device, the identifier list including one or more identifiers, arranged according to a predetermined rule, that each correspond to a different valid or revoked device, receives range information indicating a target range from the information usage device, the target range, which is specified using the identifier list, including a target identifier corresponding to the information usage device, and uses the received range information in judging whether the information usage device is valid or revoked.

17. The input/output device of claim 16, comprising:

an acquiring unit operable to acquire the identifier list from an external source;

an output unit operable to output the acquired identifier list to the information usage device;

an ID receiving unit operable to receive from the information usage device, the target identifier and, as the range information, one or more identifiers, extracted from the identifier list by the information usage device, that are included within the target range; and

a judging unit operable to judge whether the information usage device is valid or revoked, depending on whether the received target identifier matches any of the identifiers received as the range information, and to suppress the information input/output if the information usage device is judged to be revoked.

18. The input/output device of claim 17, wherein

the target identifier identifies a public-key certificate certifying the authenticity of a public key of the information usage device,

each identifier in the identifier list identifies a public-key certificate of a different revoked device, and

the judging unit judges the information usage device to be revoked if the target identifier matches any of the one or more extracted identifiers, and to be valid if the target identifier does not match any of the one or more extracted identifiers.

19. The input/output device of claim 18, wherein

the identifier list has arranged therein according to the predetermined rule, certification data that certifies, with respect to each of one or more ranges, the authenticity of the one or more identifiers included within the range, the ID receiving unit receives from the information usage device, certification data, extracted from the identifier list by the information usage device, that certifies the authenticity of the one or more extracted identifiers, and

the judging unit verifies the authenticity of the received certification data, and judges, if the authenticity is verified, whether the information usage device is valid or revoked.

20. The input/output device of claim 19, wherein

the extracted certification data is signature data generated by performing a digital signature on the one or more extracted identifiers, and

the judging unit stores a public key corresponding to a secret key used in generating the signature data, and uses the public key in verifying the authenticity of the signature data.

21. The input/output device of claim 19, wherein

the extracted certification data is an authenticator generated by using a 1st secret key on the one or more extracted identifiers, and

the judging unit stores a 2nd secret key that is identical to the 1st secret key, and uses the 2nd secret key in verifying the authenticity of the authenticator.

22. The input/output device of claim 17, wherein

the target identifier identifies a public-key certificate certifying the authenticity of a public key of the information usage device,

each identifier in the identifier list identifies a public-key certificate of a different valid device,

the ID receiving unit receives the target identifier and a single extracted identifier, and

the judging unit judges the information usage device to be valid if the target and extracted identifiers match, and to be revoked if the target and extracted identifiers do not match.

23. The input/output device of claim 22, wherein

the identifier list has arranged therein one or more pieces of certification data, each corresponded to and certifying the authenticity of a different one of the identifiers,

the ID receiving unit receives from the information usage device, certification data, extracted from the identifier list by the information usage device, that certifies the authenticity of the extracted identifier, and

the judging unit verifies the authenticity of the received certification data, and judges, if the authenticity is verified, whether the information usage device is valid or revoked.

24. The input/output device of claim 17, wherein

the target identifier is included in a public-key certificate certifying the authenticity of a public key of the information usage device,

each identifier in the identifier list is included in a public-key certificate of a different valid or revoked device, and

the ID receiving unit receives from the information usage device, the target identifier, and two extracted identifiers defining the target range, which is a range showing the public-key certificates of one of valid or revoked devices, and

the judging unit judges whether the information usage device is valid or revoked, depending on whether the target identifier is included within the range defined by the two extracted identifiers.

25. The input/output device of claim 17, further comprising:

an information output unit operable to securely output usage information to the information usage device, if the information usage device is judged to be valid.

26. The input/output device of claim 25, wherein

the ID receiving unit receives a public key of the information usage device, and

the information output unit uses the received public key in encrypting the usage information to generate encrypted usage information, and outputs the encrypted usage information to the information usage device.

27. The input/output device of claim 17, further comprising:

an ID storage unit operable to store a certificate identifier that identifies a public-key certificate certifying the authenticity of a public key of the input/output device; and

an ID output unit operable to output the certificate identifier to the information usage device.

28. The input/output device of claim 27, further comprising:

a processing unit operable to establish a secure communication channel between the input/output device and the information usage device, if the information usage device is judged to be valid; and

an information output unit operable to securely output usage information to the information usage device, if the secure communication channel is established.

29. The input/output device of claim 28, wherein

the processing unit judges that a secure communication channel has been established if a shared key is generated between the information usage and input/output devices, and

the information output unit encrypts the usage information using the shared key to generate encrypted usage information, and outputs the encrypted usage information to the information usage device.

30. An information usage device that performs information input/output via an input/output device, and, when instructed by the input/output device, performs part of processing for judging whether the information usage device is one of valid and revoked.

31. The information usage device of claim 30 receives an identifier list from the input/output device, the identifier list including one or more identifiers, arranged according to a predetermined rule, that each correspond to a different validor revokeddevice, and, as part of the judgment processing, uses the received identifier list in specifying a target range that includes a target identifier stored by the information usage device, and outputs range information indicating the specified target range to the input/output device.

32. The information usage device of claim 31, comprising:

a storage unit operable to store the target identifier, which corresponds to the information usage device;

a receiving unit operable to receive the identifier list from the input/output device;

an extracting unit operable to use the received identifier list in specifying the target range, and to extract all of the identifiers included within the specified target range from the identifier list; and

a data output unit operable to output to the input/output device the target identifier and the one or more identifiers extracted as the range information.

33. The information usage device of claim 32, wherein

the extracting unit specifies the target range from one or more ranges each defined by two identifiers arranged consecutively in the identifier list, and extracts the two identifiers defining the specified target range, and

the data output unit outputs to the input/output device the target identifier and the two identifiers extracted as the range information.

34. The information usage device of claim 32, wherein

the target identifier identifies a public-key certificate certifying the authenticity of a public key of the information usage device,

each identifier in the identifier list identifies a public-key certificate of a different revoked device, and

the extracting unit extracts in the arranged order, the one or more identifiers included within the specified target range.

35. The information usage device of claim 34, wherein

the identifier list has arranged therein according to the predetermined rule, certification data that certifies, with respect to each of one or more ranges, the authenticity of the one or more identifiers included within the range,

the extracting unit extracts from the identifier list, the certification data certifying the authenticity of the one or more extracted identifiers, and

the data output unit outputs the extracted certification data to the input/output device.

36. The information usage device of claim 35, wherein the extracted certification data is signature data generated by performing a digital signature on the one or more extracted identifiers.

37. The information usage device of claim 35, wherein the extracted certification data is an authenticator generated

by using a common secret key that is identical to a secret key of the input/output device on the one or more extracted identifiers.

38. The information usage device of claim 32, wherein

the target identifier identifies a public-key certificate certifying the authenticity of a public key of the information usage device,

each identifier in the identifier list identifies a public-key certificate of a different valid device, and

the extracting unit judges whether any of the identifiers in the identifier list match the target identifier, and extracts the matching identifier if judged in the affirmative.

39. The information usage device of claim 38, wherein

the identifier list has arranged therein one or more pieces of certification data, each corresponded to and certifying the authenticity of a different one of the identifiers,

the extracting unit extracts the certification data corresponding to the extracted identifier, and

the data output unit outputs the extracted certification data to the input/output device.

40. The information usage device of claim 32, wherein

the target identifier is included in a public-key certificate certifying the authenticity of a public key of the information usage device,

each identifier in the identifier list is included in a public-key certificate of a different valid or revoked device, and

the extracting unit specifies the target range, which is a range showing the public-key certificates of one of valid or revoked devices, and extracts the two identifiers defining the specified target range.

41. The information usage device of claim 32, further comprising:

a usage unit operable to securely receive usage information from the input/output device if judged by the input/output device that the information usage device is valid, and to use the received usage information.

42. The information usage device of claim 41, wherein

the usage information was encrypted in the input/output device using a public key of the information usage device, and

the usage unit stores a secret key corresponding to the public key, and on receipt of the encrypted usage information from the input/output device, decrypts the encrypted usage information using the secret key to generate usage information and uses the generated usage information.

43. The information usage device of claim 32, further comprising:

an ID reception unit operable to receive from the input/output device a certificate identifier that identifies a public-key certificate certifying the authenticity of a public key of the input/output device;

a list receiving unit operable to receive a revocation list via the input/output device, the revocation list including one or more revoked identifiers that each identify a public-key certificate of a different revoked device; and

an ID judging unit operable to judge whether the input/output device is valid or revoked, depending on whether the received certificate identifier matches any of the revoked identifiers included in the revocation list.

44. The information usage device of claim 43, further comprising:

a processing unit operable to establish a secure communication channel between the information usage device and the input/output device, if the input/output device is judged to be valid; and

a usage unit operable to securely receive usage information from the input/output device if the secure communication channel is established, and to use the received usage information.

45. The information usage device of claim 44, wherein

the processing unit judges that a secure communication channel has been established if a shared key is generated between the information usage and input/output devices,

the usage information was encrypted in the input/output device using the shared key, and

the usage unit, on receipt of the encrypted usage information from the input/output device, decrypts the encrypted usage information using the shared key and uses the generated usage information.

46. A list generation device for generating an identifier list that includes one or more identifiers corresponding to one or more valid or revoked devices, comprising:

a list storage unit;

an acquiring unit operable to acquire one or more identifiers; and

a generating unit operable to arrange the acquired identifiers according to a predetermined rule to generate an identifier list that includes the arranged identifiers, and to write the generated identifier list to the list storage unit.

47. The list generation device of claim 46, wherein

each identifier in the identifier list identifies a public-key certificate of a different revoked device, and

the generating unit includes:

a key storage subunit operable to store a secret key;

an arranging subunit operable to arrange the acquired identifiers according to the predetermined rule;

a data generating subunit operable to extract, in the arranged order of the identifiers, one or more identifiers constituting a range, and to use the secret key in generating certification data that certifies the authenticity of the one or more extracted identifiers;

a control subunit operable to control the data generating subunit to repeat the identifier extraction and the data generation, until the data generation has been completed for all of the identifiers; and

a list generating subunit operable, after the completion of the data generation for all of the identifiers, to generate an identifier list that includes the arranged identifiers and the generated certification data arranged according to the predetermined rule, and to write the generated identifier list to the list storage unit.

48. The list generation device of claim 46, wherein

each identifier in the identifier list identifies a public-key certificate of a different valid device, and

the generating unit includes:

a key storage subunit operable to store a secret key;

a data generating subunit operable to use the secret key in performing a digital signature on each of the acquired identifiers to generate certification data certifying the authenticity of the identifier; and

a list generating unit operable to generate an identifier list in which the arranged identifiers are corresponded with respective pieces of the generated certification data, and to write the generated identifier list to the list storage unit.

49. A machine-readable recording medium comprising a list storage unit operable to store an identifier list that includes one or more identifiers, arranged according to a predetermined rule, that each correspond to a different valid or revoked device.

50. The recording medium of claim 49, wherein

each identifier in the identifier list identifies a public-key certificate of a different revoked device, and

the identifier list has arranged therein according to the predetermined rule, certification data that certifies, with respect to each of one or more ranges, the authenticity of the one or more identifiers included within the range.

51. The recording medium of claim 49, wherein

each identifier in the identifier list identifies a public-key certificate of a different valid device, and

the identifier list has arranged therein according to the predetermined rule, one or more pieces of certification data, each corresponded to and certifying the authenticity of a different one of the identifiers.

52. An identifier list that includes one or more identifiers, arranged according to a predetermined rule, that each correspond to a different valid or revoked device.

53. The identifier list of claim 52, wherein

each identifier corresponds to a revoked device, and

the identifier list has arranged therein according to the predetermined rule, certification data that certifies, with respect to each of one or more ranges, the authenticity of the one or more identifiers included within the range.

54. The identifier list of claim 52, wherein

each identifier corresponds to a valid device, and the identifier list has arranged therein according to the predetermined rule, one or more pieces of certification data, each corresponded to and certifying the authenticity of a different one of the identifiers.

55. An information input/output system comprising:

an input/output device; and

application software for performing information input/output via the input/output device, wherein

the input/output device has the application software perform part of processing for judging whether the application software is one of valid and revoked.

56. A judging method used in an input/output device via which an information usage device performs information input/output, comprising the steps of:

outputting an identifier list to the information usage device, the identifier list including one or more identifiers, arranged according to a predetermined rule, that each correspond to a different valid or revoked device;

receiving range information from the information usage device, the range information showing a target range, specified using the identifier list, that includes a target identifier corresponding to the information usage device; and using the received range information in judging whether the information usage device is one of valid and revoked.

57. A judging computer program used in an input/output device via which an information usage device performs information input/output, comprising the steps of:

outputting an identifier list to the information usage device, the identifier list including one or more identifiers, arranged according to a predetermined rule, that each correspond to a different valid or revoked device;

receiving range information from the information usage device, the range information showing a target range, specified using the identifier list, that includes a target identifier corresponding to the information usage device; and

using the received range information in judging whether the information usage device is one of valid and revoked.

58. A machine-readable recording medium storing a judging computer program used in an input/output device via which an information usage device performs information input/output, the computer program comprising the steps of:

outputting an identifier list to the information usage device, the identifier list including one or more identifiers, arranged according to a predetermined rule, that each correspond to a different valid or revoked device;

receiving range information from the information usage device, the range information showing a target range, specified using the identifier list, that includes a target identifier corresponding to the information usage device; and

using the received range information in judging whether the information usage device is one of valid and revoked.

59. An information-specifying method used in an information usage device that performs information input/output via an input/output device, comprising the steps of:

receiving an identifier list from the input/output device, the identifier list including one or more identifiers, arranged according to a predetermined rule, that each correspond to a different valid or revoked device;

using the received identifier list in specifying a target range that includes a target identifier stored by the information usage device; and

outputting range information that indicates the specified target range to the input/output device.

60. An information-specifying computer program used in an information usage device that performs information input/output via an input/output device, comprising the steps

of:

receiving an identifier list from the input/output device, the identifier list including one or more identifiers, arranged according to a predetermined rule, that each correspond to a different valid or revoked device;

using the received identifier list in specifying a target range that includes a target identifier stored by the information usage device; and

outputting range information that indicates the specified target range to the input/output device.

61. A machine-readable recording medium storing an information-specifying computer program used in an information usage device that performs information input/output via an input/output device, the computer program comprising the steps of:

receiving an identifier list from the input/output device, the identifier list including one or more identifiers, arranged according to a predetermined rule, that each correspond to a different valid or revoked device;

using the received identifier list in specifying a target range that includes a target identifier stored by the information usage device; and

outputting range information that indicates the specified target range to the input/output device.